Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 58 (2015) 755 – 762

Procedia Computer Science

Second International Symposium on Computer Vision and the Internet (VisionNet'15)

Performance Evaluation of Non Sinusoidal Wavelets for Partial Image Scrambling Using Kekre's Walsh Sequency

Tanuja Sarode[a], Pallavi N Halarnkar[b]*

[a]*Associate Professor, TSEC, Mumbai University,Mumbai 400050, India,*
[b]*Assistant Professor/PhD Research Scholar, MPSTME, NMIMS University,Mumbai 400056, India*

Abstract

Image security is an important aspect in Digital image processing. There are number of ways of securing digital data. The most common form being, the scrambling or encryption method. In this paper, Partial image scrambling method is proposed using Non Sinusoidal wavelets, the image is scrambled in the wavelet domain using Kekre's Walsh Sequency algorithm and then an inverse transform is applied to get the scrambled image in spatial domain. The scrambling in wavelet domain helps resists against statistical attacks. From the experimental results it can be seen that in cases where L component of the wavelet is included the scrambled image performs better. The choice in components for scrambling helps achieve good compression hence reduces the computations required. The best performers are the Kekre and Slant Wavelet.

Keywords: Kekre's Walsh Sequency;Scrambling; Non Sinusoidal Wavelets

1. Introduction

In the recent years the amount of digital data has increased, which includes text and multimedia like digital images, this data need to be protected or secured from intruders. As we know digital images are huge in size, they contain a lot of redundancies, these redundancies could be removed and only useful image pixels can be scrambled this will not only reduce the computations but also save the bandwidth when transferred across internet. CharlesD.Creusere et al. [1] proposed an image scrambling algorithm based on polyphase filter banks which is a modification to the classic time frequency permutation method, the method helps reducing the time and memory requirements without reducing its performance. Min Li proposed a multi-region based image scrambling algorithm using Arnold

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: author@institute.xxx

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)
doi:10.1016/j.procs.2015.08.097

transformation [2]. The transformation is applied on image blocks a method proposed by Zhenwei Shang et al. [16]. A simple image scrambling algorithm for image based authentication is proposed by Giaime Ginesu et al. [3]. The said method is implemented in wavelet based domain. The method is extended to mobile based applications [4]. Sandeep Kaur et al. proposed a novel four level image encryption method based on hash [5]. A new measure of image scrambling degree is proposed by Xiongjun Li [6]. The proposed measure is based on grey level differences and information entropy. The measure is applied to scrambled images obtained using different methods. Scrambling degree based on statistical Hypothesis testing is proposed by Zhiwei Li et al. [7]. The measure is based on chi-square goodness of fit test. Shujun Li et al. [8] offered cryptanalysis on an encryption scheme without bandwidth expansion. The scrambling method was based on 2D discrete prolate spheroidal sequences (DPSS). Multi-dimensional Orthogonal Transform sequence is used for image scrambling, Shuhong L. et al. [9]. The method is very robust as the keys are the conditions used to generate the sequence. The problem of scrambling non equilateral images is addressed by Shao Liping et al. [10]. The method is based on Random shuffling strategy and computes the shifting path using low cost. Shao Liping et al. proposed a scrambling matrix generation algorithm for image scrambling [11], the method has low cost of generation and wide space for matrix generation which increases security. Prashan Premaratne et al. [12] proposed a random key based image scrambling, the method uses a random key and shuffling the pixels row and column wise based on the key. The scrambling degree of a Binary image using bipartite graph and its degree is introduced by Fuai-ying et al. [13]. Abhijeet A. Ravankar, [14] proposed a New Linear Transform for image scrambling. Both blocked and scalar cases have been considered. Image scrambling and encryption algorithm is proposed by Zhang Ruihong et al.[15]. The method makes use of limited finite integer domain.it includes both gray as well as position transformation. KokSheik Wong et al. [17] proposed an extension to Scascra method for image scrambling. The method scrambles the diagonal blocks so as to achieve scan like effect on the scrambled image. A study on Fibonacci periodicity is given by Weigang Zou et al. [18]. The transformation is also used for image scrambling. Yicong Zhou et al.[19] gave a P-code Fibonacci technique for image scrambling and a comparison of these sequences along with some others is discussed [20], the methods are compared based on data loss attacks, noise attacks and plain text attacks. Wavelet Generation using Kronecker Product

For Wavelet generation of Sinusoidal Wavelet, Kronecker Product method is used. The image size used for experimental purpose is 256x256. Hence to generate a wavelet transform, the transform matrix of size 16x16 is used. The Kronecker Product of the matrix is taken with itself to generate a wavelet having four components LL, LH, HH and HL. The Kronecker Product can be applied as follows

$$A \otimes A = aij\,[A] \tag{1}$$

Where size of A is 16x16 and is used to generate a wavelet transform of size 256x256.

$$\boxed{\begin{matrix} \text{A} \\ \text{(16x16)} \end{matrix}} \otimes \boxed{\begin{matrix} \text{A} \\ \text{(16x16)} \end{matrix}} = \begin{array}{|c|c|} \hline \text{LL} & \text{LH} \\ \hline \text{HL} & \text{HH} \\ \hline \end{array}$$

Wavelet(256X256)

Fig. 1. An Example of Wavelet Generation

In the above Figure 1. LL represents the component with maximum energy of the original image, LH, HH and HL represents the components with some amount of image energy.

The above concept is used to generate the non-sinusoidal wavelets, the transforms used are Kekre transform, Walsh Transform, Haar Transform and Slant transform [21].

2. Proposed Approach for Partial Image Scrambling

The Figure below explains the step by step procedure used for scrambling image using Walsh sequency in wavelet domain. Figure 2(a) shows the scrambling process and (b) shows the all the different combinations that are used for scrambling the image in wavelet domain using Kekre's Walsh Sequency [22].The proposed approach focuses towards partial image scrambling. The Walsh sequency is applied on all the combinations of wavelet components , so as to do an in depth study of which components of wavelet (i.e. LL, LH, HH and HL) results in a higher error in the resultant image. The different combinations explored for the proposed approach includes (1) LL,LH,HH & HL (2) LL, LH, HH (3) LL,LH,HL (4) LL,HH,HL (5) LL,LH (6) LL, HH (7) LL, HL(8) LL. For e.g.

(2) LL, LH and HH (HL component is removed from the wavelet domain and only LL,LH and HH components are scrambled by applying Walsh sequency), which reduces the computational complexity in the scrambling and descrambling process , as compared to the traditional approach in which the scrambling and descrambling process needs to be applied to all the pixels of the image in the spatial domain.

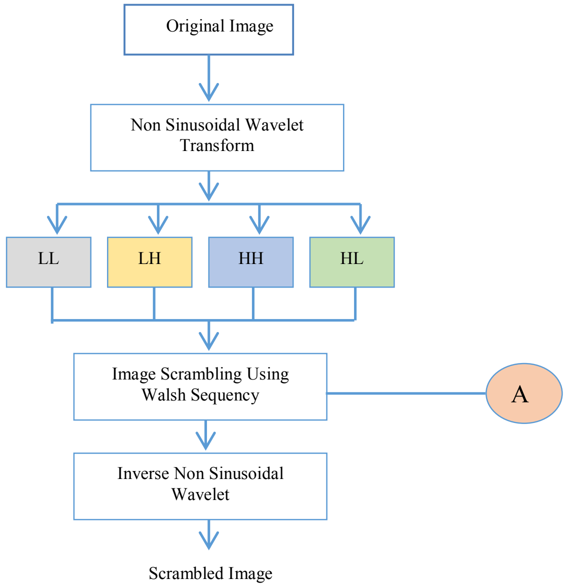


Fig. 2 (a) Scrambling Process

1	**LL**	**LH**	**HH**	**HL**
2	**LL**	**LH**	**HH**	**0**
3	**LL**	**LH**	**0**	**HL**
4	**LL**	**0**	**HH**	**HL**
5	**LL**	**LH**	**0**	**0**
6	**LL**	**0**	**HH**	**0**
7	**LL**	**0**	**0**	**HL**
8	**LL**	**0**	**0**	**0**

A

Fig. 2 (b) Different combinations of Components scrambled

4. Experimental Results

For experimental purpose 15 (24 bit color) images of size 256x256 were used. The results displayed below are averaged over fifteen images. The parameters used for experimental analysis used include Adjacent row pixel correlation (ARPC), Adjacent column pixel correlation (ACPC), Adjacent diagonal pixel correlation (ADPC), Adjacent anti diagonal pixel correlation(AADPC), Structural similarity index measure (SSIM), Peak average fractional change in pixel value (PAFCPV)[23] and Mean Squared Error(MSE). Figure 3, shows the different scrambled images obtained for scrambling different combinations of wavelet components for Kekre Wavelet. Figure 3(a) shows the original image, (b)–(e) & (j)-(m) shows the scrambled images, (f)-(i) &(n)-(q) shows the descrambled images. Figure 4 to 7 (a) Shows the Reduction in correlation obtained in row, column, diagonal and anti-diagonal pixels, (b) shows the structural similarity index measure, (c) shows the Peak average fractional change in pixel value, and (d) shows the Mean squared error for Walsh, Slant, Kekre and Haar Wavelet.

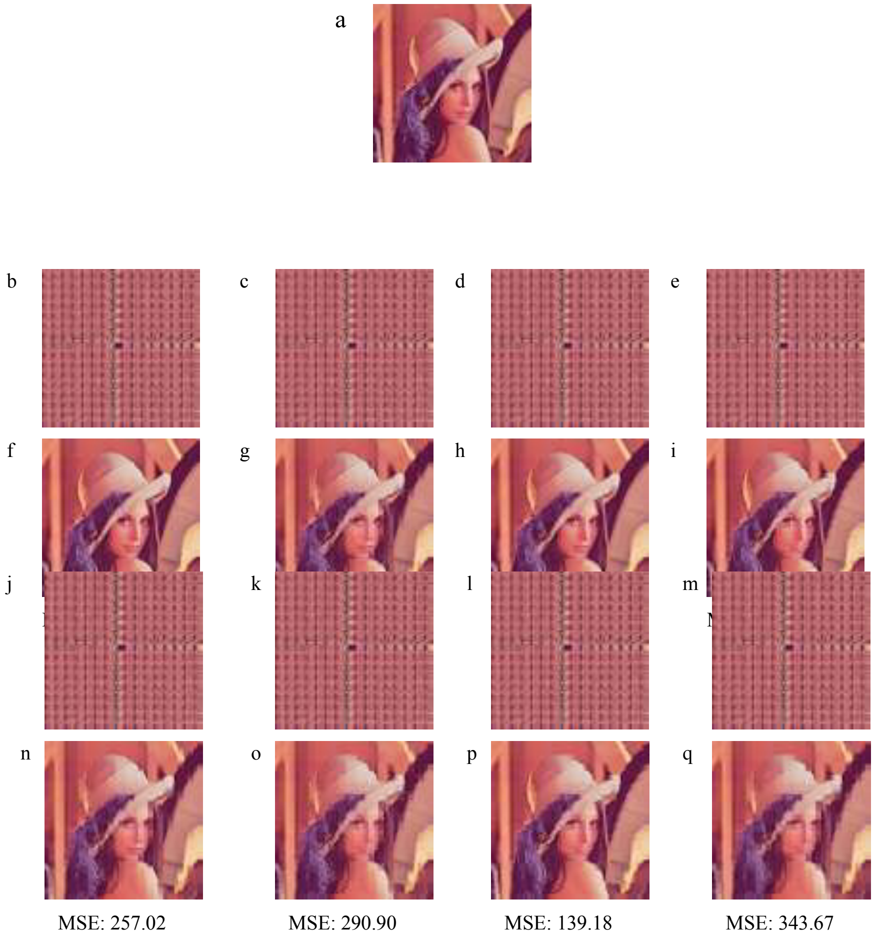
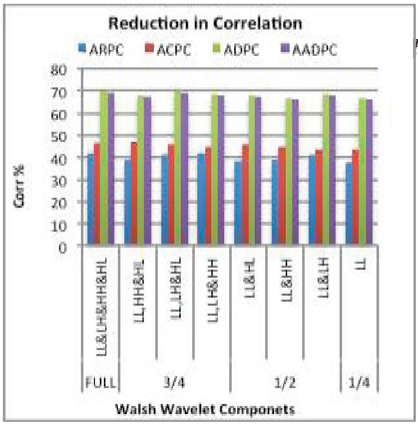


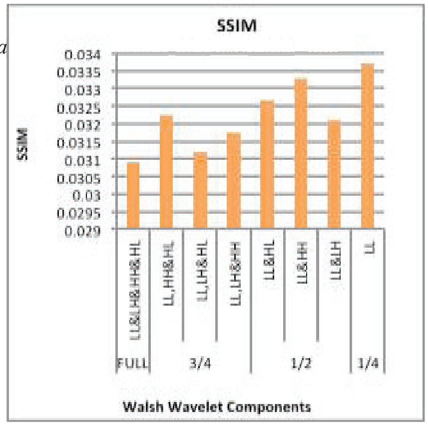
Figure 3. Kekre Wavelet Domain with Walsh Sequency
(a)Original Image, scrambled images for (b) LL,LH,HH & HL (c) LL, LH, HH (d) LL,LH,HL (e) LL,HH,HL , descrambled images (f)-(i), scrambled images for (j) LL,LH (k) LL, HH (l) LL, HL(m) LL, descrambled images (n)-(q)

a

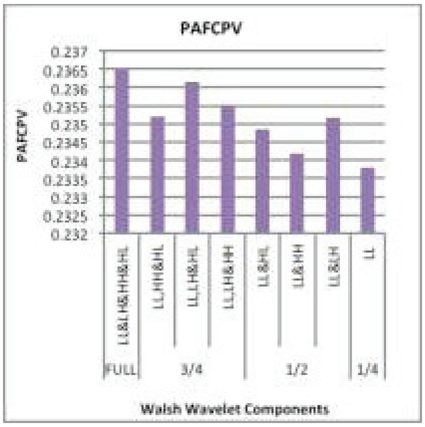


b

Procedia



c



d

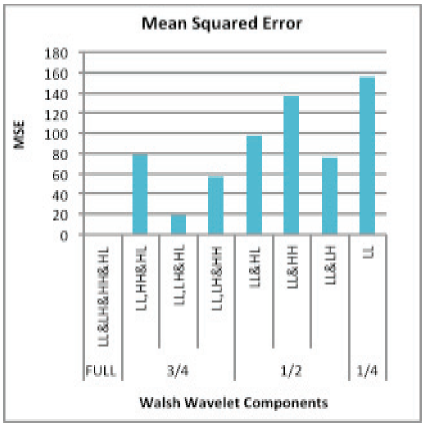
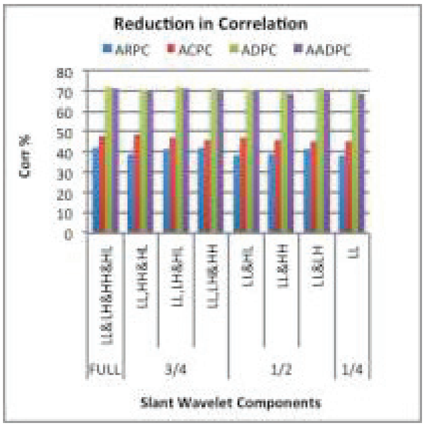
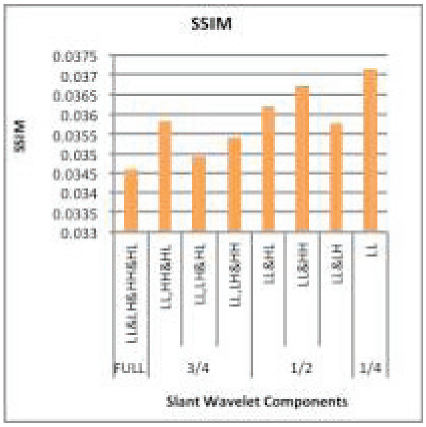


Figure 4. Walsh Wavelet Domain with Walsh Sequency
(a) Reduction in Correlation in scrambled images, (b) Structural Similarity Index Measure in scrambled images (c) Peak average fractional change in pixel value in scrambled images and (d) Mean squared error in Descrambled images for Walsh wavelet

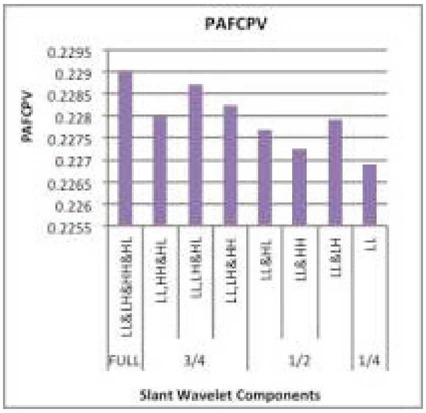
a



b



c



d

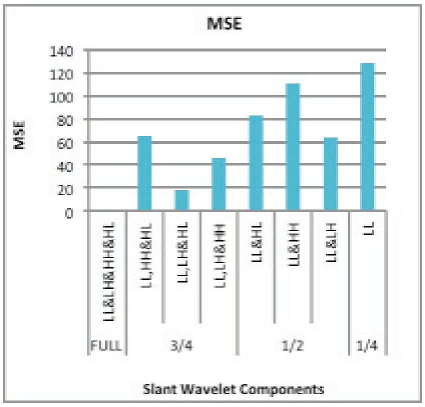
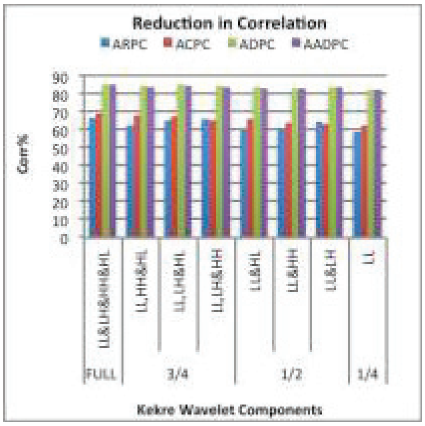
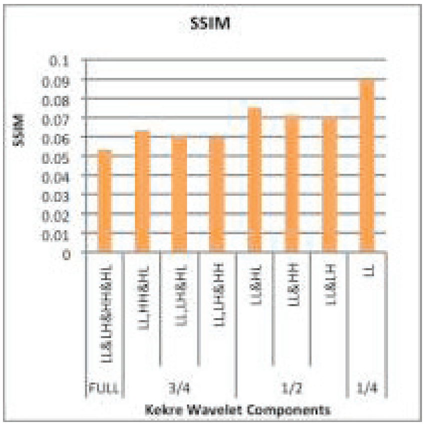


Figure 5. Slant Wavelet Domain with Walsh Sequency
(a) Reduction in Correlation in scrambled images, (b) Structural Similarity Index Measure in scrambled images (c) Peak average fractional change in pixel value in scrambled images and (d) Mean squared error in Descrambled images for Walsh wavelet

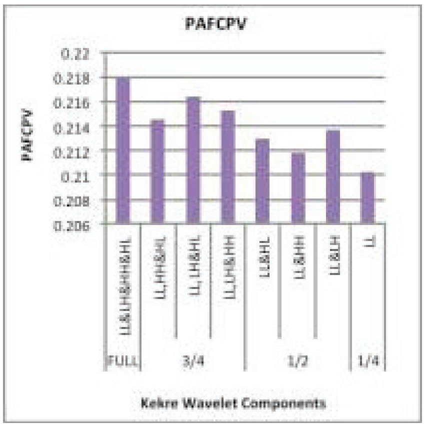
a



b



c



d

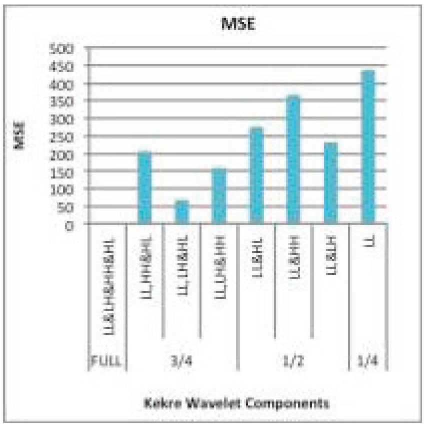


Figure 6. Kekre Wavelet Domain with Walsh Sequency
(a) Reduction in Correlation in scrambled images, (b) Structural Similarity Index Measure in scrambled images (c) Peak average fractional change in pixel value in scrambled images and (d) Mean squared error in Descrambled images for Walsh wavelet

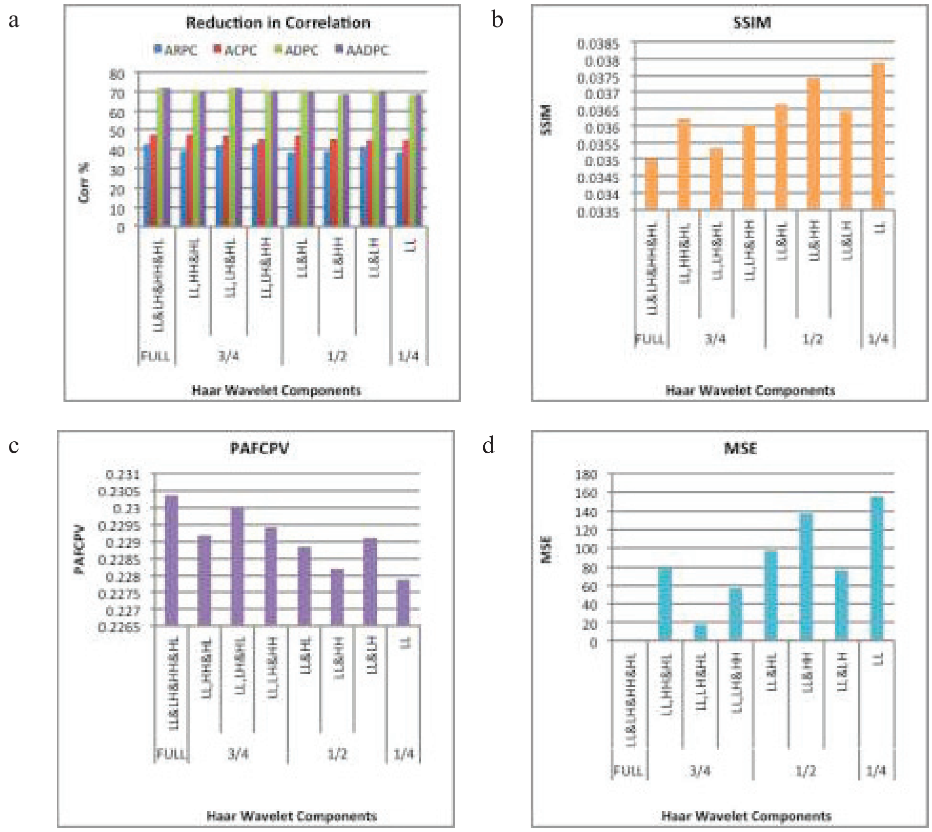


Figure 7. Haar Wavelet Domain with Walsh Sequency
(a) Reduction in Correlation in scrambled images, (b) Structural Similarity Index Measure in scrambled images (c) Peak average fractional change in pixel value in scrambled images and (d) Mean squared error in Descrambled images for Walsh wavelet

5. Conclusion

In this paper a novel approach for partial image scrambling is proposed. The performance evaluation of all the non sinusoidal wavelets is carried out. There are 4 categories which are been considered and evaluated for scrambling process. Based on different parameters it can be observed that the first category i.e. scrambled image containing all the four components LL, LH, HH and HL performs the best, it gives the highest reduction in correlation, lowest SSIM is obtained , highest value of PAFCPV is obtained and zero MSE is obtained for all the Wavelet when compared to other categories. Kekre Wavelet Transform gives the highest reduction in correlation a value of 85%. Minimum MSE is obtained in Slant Wavelet. However scrambling needs to be applied to all the four components of Wavelet. In case compression is to be achieved the other categories may be considered i.e. ¾ , ½ and ¼ . In ¾ and ½ categories it is observed that the scrambled image with maximum L component gives good results. Hence based on MSE it can be decided as to which of the category may be chosen for image scrambling by reducing the computations. In spatial domain when any scrambling technique is applied it needs (255+255) shuffling computations. i.e. 255 shuffling for rows and 255 shuffling for column pixels, however our partial image scrambling category of ¾ and ½ reduces these computations as we don't consider all the pixels for shuffling in wavelet domain.

References

1. Creusere, Charles D., and Sanjit K. Mitra. Efficient image scrambling using polyphase filter banks. In: Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference,1994, 2, 81-85. IEEE.
2. Li, Min, Ting Liang, and Yu-jie He. Arnold Transform Based Image Scrambling Method. In: 3rd International Conference on Multimedia Technology. 2013.

3. Ginesu, Giaime, Daniele D. Giusto, and Tatiana Onali. Wavelet domain scrambling for image-based authentication. In : Acoustics, Speech and Signal Processing, ICASSP 2006 IEEE International Conference on, 2, II. IEEE, 2006.
4. Ginesu, Giaime, Tatiana Onali, and Daniele D. Giusto. Efficient Scrambling of Wavelet-based Compressed Images: A comparison between simple techniques for mobile applications. In: Proceedings of the 2nd international conference on Mobile multimedia communications, 43. ACM, 2006.
5. Sandeep Kaur and Sumeet Kaur.Four Level Image encryption using scrambling and key based methods, *J. IJCSC*, Vol 3. No 1,187-190, 2012
6. Li, Xiongjun. A new measure of image scrambling degree based on grey level difference and information entropy. In: Computational Intelligence and Security. CIS'08. International Conference on, 1, 350-354. IEEE, 2008.
7. Li, Zhiwei, and Xiyang Yang. A new measure of image scrambling degree based on statistical hypothesis testing. In: Image and Signal Processing (CISP), 3rd International Congress on, 5, 2409-2413. IEEE, 2010.
8. Li, Shujun, Chengqing Li, Kwok-Tung Lo, and Guanrong Chen. Cryptanalysis of an image scrambling scheme without bandwidth expansion. Circuits and Systems for Video Technology, IEEE Transactions on 18. 3. 338-349. 2008
9. Li, Shuhong, Junmin Wang, and Xing Gao. The fast realization of image scrambling algorithm using multi-dimensional orthogonal transform. In :Image and Signal Processing, 2008. CISP'08. Congress on. 3. 47-51. IEEE, 2008.
10. Liping, Shao, Qin Zheng, Liu Bo, Qin Jun, and Li Huan. Image scrambling algorithm based on random shuffling strategy. In :Industrial Electronics and Applications. ICIEA 2008. 3rd IEEE Conference on. 2278-2283. IEEE.2008.
11. Liping, Shao, Qin Zheng, Li Huan, Qin Jun, and Liu Bo. Scrambling matrix generation algorithm for high dimensional image scrambling transformation. In: Industrial Electronics and Applications. ICIEA 2008. 3rd IEEE Conference on. 1707-1712. IEEE. 2008.
12. Premaratne, Prashan, and Malin Premaratne. Key-based scrambling for secure image communication. In Emerging Intelligent Computing Technology and Applications. 259-263. Springer Berlin Heidelberg, 2012.
13. Ai-ying, Fu, Zeng Qing-wei, Xu Zhi-hai, and Deng Geng-sheng. Binary image scrambling evaluation method based on the mean square deviation and the bipartite graph. In: Computer Communication Control and Automation (3CA), 2010 International Symposium on.1. 237-239. IEEE, 2010.
14. Ravankar, Abhijeet A., and Stanislav G. Sedukhin. Image scrambling based on a new linear transform. In Multimedia Technology (ICMT), 2011 International Conference on. 3105-3108. IEEE, 2011.
15. Zhang, Ruihong, and Zhichao Yu. Image Scrambling Encryption Algorithm Based on Limited Integer Domain. In: Proceedings of the 2010 International Symposium on Intelligence Information Processing and Trusted Computing. 693-696. IEEE Computer Society, 2010.
16. Shang, Zhenwei, Honge Ren, and Jian Zhang. A block location scrambling algorithm of digital image based on Arnold transformation. In: Young Computer Scientists. ICYCS 2008. The 9th International Conference for. 2942-2947. IEEE, 2008
17. Wong, KokSheik, and Kiyoshi Tanaka. Scalable image scrambling method using unified constructive permutation function on diagonal blocks. In:Picture Coding Symposium (PCS), 2010.138-141. IEEE, 2010.
18. Zou, Weigang, Jiangyan Huang, and Caiying Zhou.Digital image scrambling technology based on two dimension Fibonacci transformation and its periodicity.2010. 415-418.
19. Zhou, Yicong, Sos Agaian, Valencia M. Joyner, and Karen Panetta. Two Fibonacci p-code based image scrambling algorithms. In: Electronic Imaging 2008. 681215-681215. International Society for Optics and Photonics, 2008.
20. Zhou, Yicong, Karen Panetta, and Sos Agaian. Comparison of recursive sequence based image scrambling algorithms. In: Systems, Man and Cybernetics, SMC 2008. IEEE International Conference on. 697-701. IEEE. 2008.
21. H.B.Kekre, Tanuja Sarode, Pallavi N. Halarnkar, Image Scrambling Using non Sinusoidal Transforms and key Based Scrambling Technique. J. International Journals of Computers and Technology, 12(8) . 3809-3822.
22. Kekre, H. B, Tanuja K Sarode, and Jagruti K Save. New Clustering Algorithm for Vector Quantization using Walsh Sequence. J. *International Journal of Computer Applications* 39, 1 (2012): 4-9.
23. Kekre, H. B., Tanuja Sarode, and Pallavi N. Halarnkar. Chaotic Truncated Sine Series with MOD operator for Image Encryption. In: Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, 31. ACM, 2014.